UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/634,841	08/08/2000	Takuya Wada	SON-1887	4733

7590 01/21/2005	EXAMINER	
RADER, FISHMAN & GRAUER, P.L.L.C.	DINH, MINH	
Suite 501		
1233 20th Street, NW	ART UNIT	PAPER NUMBER
Washington, DC 20036	2132	

DATE MAILED: 01/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *Th MAILING DATE of this communication appears on the cover she t with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _16 August 2004_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _21-58_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _21-30,32-33,35-48,50-51 and 53-58_ is/are rejected.

7)☒ Claim(s) _31,34,49 and 52_ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _08 August 2000_ is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   This action is in response to the amendment filed 08/16/2004. Claims 1-20 have been canceled and claims 21-58 have been added. The specification has also been amended.

2.   The objections to the drawings and the specification in the previous Office Action have not been addressed in the amendment. Applicant is reminded to respond to these objections in the next reply.

Response to Arguments

3.   Applicant's arguments filed 08/16/2004 have been fully considered but they are not persuasive. Applicant argues that Borza fails to disclose generating a binary image from the gray scale image, a binary image pixel of the binary image being generated by comparing the gray scale pixel value with an average of gray scale pixel values for the plurality of pay scale pixels, the binary image pixel having a binary pixel value expressed by a single bit. Borza discloses a process which compares each grey scale pixel value of a grey scale image with an average of gray scale pixel values for the plurality of gray scale pixels and generates a binary value expressed by a single bit based on the comparison (col. 4, line 63 – col. 5, line 3). Since Borza process performs the exact same steps as those in the applicant's process of generating a binary image

from the gray scale image, the result of Borza process meets the limitation of a binary

image.

Drawings

4.   The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5)

because they include the following reference sign(s) not mentioned in the description:

reference numeral "100" (figure 1). A proposed drawing correction, corrected drawings,

or amendment to the specification to add the reference sign(s) in the description, are

required in reply to the Office action to avoid abandonment of the application. The

objection to the drawings will not be held in abeyance.

5.   The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5)

because they do not include the following reference numerals mentioned in the

description: "6" (see page 15, third line from bottom) and "56" (page 19, line 11). A

proposed drawing correction or corrected drawings are required in reply to the Office

action to avoid abandonment of the application. The objection to the drawings will not

be held in abeyance.

Specification

6.   The title of the invention is not descriptive. A new title is required that is clearly

indicative of the invention to which the claims are directed.

The following title is suggested: "Random Number Generation Apparatus And Random Number Generation Method Using Ambient Light".

7.   Claim 37 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The limitation of the claim, "said encryption key is according to said random number sequence" does not constitute a further limitation with regard to the limitation of the parent claim, "said encryption key is said random number sequence". For examination purpose, claim 37 is treated as being dependent on claim 35.

Claim Objections

8.   Claims 27, 31, 34, 45, 49 and 52 are objected to because of the following informalities:

Regarding claims 27 and 45, "a segment of said grey scale" (lines 2-3) should be changed to "a segment of said grey scale image".

Regarding claims 31 and 49, "said plurality grey scale" (last line) should be changed to "said plurality of grey scale pixels".

Regarding claims 34 and 52, "said plurality binary" (last line) should be changed to "said plurality of binary pixels".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

9.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

10.   Claim 28 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention. Claim 28 recites the limitation "black portions" and "the white

portions" in line 2. It is not clear which limitation in the parent claim, Claim 1, that the

black and white portions are part of. For examination purpose, they are interpreted as

"the black portions of the binary image" and "the white portions of the binary image"

(Specification, fig. 3).

Claim Rejections - 35 USC § 103

11.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

12.   Claims 21 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Borza et al (6,215,874) in view of Tomko et al (5,541,994).

Regarding claims 21 and 41, Borza discloses an apparatus comprising:

a pick-up block structurally adapted to capture living body information and to
output a pick-up signal depicting said living body information (fig. 1, element 1);

A/D converter structurally adapted to convert said pick-up signal into a gray scale
image composed of a plurality of gray scale pixels, a gray scale pixel of said plurality
gray scale of pixels having a gray scale pixel value expressed by a plurality of bits (col.
4, lines 63-65; col. 6, lines 45-51);

a image processor structurally adapted to compares each grey scale pixel value
of a grey scale image with an average of gray scale pixel values for the plurality of gray
scale pixels and generates a binary value expressed by a single bit based on the
comparison (col. 4, line 63 – col. 5, line 3). Since Borza process performs the exact
same steps as those in the applicant's process of generating a binary image from the
gray scale image, the result of Borza process meets the limitation of a binary image;
and

a random number generator structurally adapted to generate a random number
sequence from said pick-up signal when no living body information is captured by said
pick-up block, said random number sequence being generated using said binary pixel
value (fig. 4a; col. 4, lines 52-56; col. 4, line 65 – col. 5, line 3).

Although Borza does not expressly disclose an encryption block utilizing the
random number, Borza teaches using random numbers for generating private and
public keys in encryption technology (col. 2, lines 5-11). Tomko discloses an apparatus
comprising a random number generator, a cryptographic key generator that generates
keys according to data obtained from the random number, and encryption/decryption

means uses the generated keys for encrypting/decrypting messages, the apparatus

meets the limitation of an encryption block (fig. 2, elements 84, 88, 92 and 96). It would

have been obvious to one of ordinary skill in the art at the time the invention was made

to modify the apparatus of Borza such that a cryptographic key generator and

encryption/decryption means are provided to generate encryption keys according to

data obtained from the random number generator and to encrypt/decrypt messages

using the generated key, as taught by Tomko. The motivation for doing so would have

been to utilize the keys generated from the random number for encryption/decryption.

Regarding claims 22 and 42, Borza further discloses that said living body

information is a fingerprint (col. 4, lines 28-30).

Regarding claims 23 and 43, Borza further discloses that said binary image is

composed of a plurality of binary image pixels (col. 4, lines 63-65).

Regarding claim 24, Borza further discloses memory to store said gray scale

image (col. 6, lines 45-51).

Regarding claim 25, Borza further discloses memory to store said binary image

(col. 4, line 63 – col. 5, line 3).

Regarding claims 26 and 44, Borza further discloses said plurality of gray scale

pixels is the number of gray scale pixels for the entire gray scale image (col. 4, lines 63-

65).

Regarding claims 27 and 45, Borza further discloses said plurality of gray scale

pixels is the number of gray scale pixels located at a segment of said gray scale image

in a predetermined range from said gray scale pixel (col. 5, lines 13-16; col. 6, lines 1-20).

Regarding claim 28, Borza further discloses that the black portions of the binary image represent convex portions of said living body information and the white portions of the binary image represent concave portions of said living body information (col. 1, line 49 – col. 2, line 4).

Regarding claims 32-33 and 50-51, Borza further discloses said binary pixel is located at a start address, said random number generator generating said random number sequence by extracting the least significant bit of said binary pixel value and the least significant bit for each of the binary pixel values of a predetermined number of binary pixels succeeding said binary pixel (col. 4, line 63 – col. 5, line 3; col. 6, lines 1-56).

Regarding claims 35, 37, 53 and 55, the encryption block discussed in claims 21 and 41 comprises encryption means to perform encryption using an encryption key according to the random number.

Regarding claims 36 and 54, Borza and Tomko do not disclose that the encryption key is the random number sequence. However, Examiner takes Official Notice that using a random number sequence as a key in DES (Data Encryption Standard) is well known in the art. It would have been obvious at the time of the invention was made to use the random number sequence as a key since Examiner takes Official Notice that using a random number sequence as a key in DES is well known in the art.

Regarding claims 39-40, 46 and 57-58, Borza discloses a pick-up block to capture a fingerprint (col. 4, lines 28-30). However, Borza does not disclose a fingerprint identification block to identify an individual by comparing said binary image with registered image information and when said individual is identified, encryption is performed using said encryption key. Tomko discloses an apparatus comprising a fingerprint identification block to identify an individual by comparing said binary image with registered image information and when said individual is identified, encryption is performed using said encryption key (fig. 2). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Borza apparatus such that it includes a fingerprint identification block to identify an individual by comparing said binary image with registered image information and when said individual is identified, encryption is performed using said encryption key, as taught by Tomko. The motivation for doing so would have been to allow the use of public key encryption techniques without a subscriber knowing his private key which enhances the security of the system (col. 6, lines 59-62).

13.   Claims 29-30 and 47-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Borza in view of Tomko as applied to claims 21 and 41 above, and further in view of Nielsen. Borza discloses said grey scale pixel is located at a start address located at a predetermined position in said grey scale image (col. 6, lines 1-20); however, Borza does not discloses that said random number generator generating said random number sequence by extracting the least significant bit of said grey scale pixel

value and the least significant bit for each of the grey scale pixel values of a

predetermined number of grey scale pixels succeeding said grey scale pixel. Nielsen

discloses a random number generator generating a random number sequence by

extracting the least significant bit of a grey scale pixel value and the least significant bit

for each of the grey scale pixel values of a predetermined number of grey scale pixels

succeeding said grey scale pixel (col. 3, lines 10-21). It would have been obvious to

one of ordinary skill in the art at the time the invention was made to modify the

apparatus of Borza such that said random number generator generating said random

number sequence by extracting the least significant bit of said grey scale pixel value

and the least significant bit for each of the grey scale pixel values of a predetermined

number of grey scale pixels succeeding said grey scale pixel, as taught by Nielsen.

Potential interceptors of signal encrypted with such a random number sequence will find

it difficult, if not impossible, to determine the random number sequence (col. 1 lines 52-

59).

14.   Claims 38 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Borza in view of Tomko as applied to claims 37 and 55 above, and further in view

of Schneier ("Applied Cryptography"). Borza discloses using the random number to

generate keys used in public key encryption (col. 2, lines 10-13). However, Borza and

Tomko do not disclose using the RSA encryption method for generating the encryption

key using two prime numbers. Schneier discloses using the RSA encryption method for

generating the encryption key using two prime numbers (section 19.3 RSA, page 467).

It would have been obvious to one of ordinary skill in the art at the time the invention

was made to modify the apparatus of Borza to use the RSA encryption method for

generating the encryption key, as taught by Schneier, because it is by far the easiest to

understand and implement (section 19.3 RSA, page 466).

Allowable Subject Matter

15.   Claims 31, 34, 49 and 52 are objected to as being dependent upon a rejected

base claim, but would be allowable if rewritten in independent form including all of the

limitations of the base claim and any intervening claims.

16.   The following is a statement of reasons for the indication of allowable subject

matter: regarding claims 31, 34, 49 and 52, the claim features of using the pixel value

of one pixel for the horizontal address and the pixel value of another pixel for the vertical

address of a start address in combination with elements of the parent claims have not

been taught by prior art.

Conclusion

17.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure:

    Chang et al, (4,225,850), discloses a non-fingerprint region indicator.

    Lee, (5,187,748), discloses an optical apparatus for fingerprint identification

system.

18.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Minh Dinh whose telephone number is 571-272-3802.

The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.
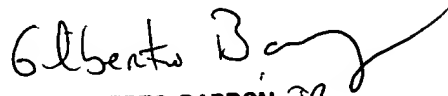
If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
1/18/05

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100